Trace-Based Control-Flow Analysis
Benoît Montagu, Thomas Jensen

To cite this version:
Benoît Montagu, Thomas Jensen. Trace-Based Control-Flow Analysis. PLDI 2021 - 42nd ACM SIGPLAN International Conference on Programming Language Design and Implementation, Jun 2021, Virtual, Canada. pp.1-15, 10.1145/3453483.3454057 . hal-03266981

HAL Id: hal-03266981
https://inria.hal.science/hal-03266981
Submitted on 22 Jun 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Trace-Based Control-Flow Analysis

Benoît Montagu
Inria
Rennes, France
benoit.montagu@inria.fr

Thomas Jensen
Inria
Rennes, France
thomas.jensen@inria.fr

Abstract

We define a small-step semantics for the untyped λ-calculus, that traces the β-reductions that occur during evaluation. By abstracting the computation traces, we reconstruct k-CFA using abstract interpretation, and justify constraint-based k-CFA in a semantic way. The abstract interpretation of the trace semantics also paves the way for introducing widening operators in CFA that go beyond existing analyses, that are all based on exploring a finite state space. We define VCFA, a widening-based analysis that limits the cycles in call stacks, and can achieve better precision than k-CFA at a similar cost.

CCS Concepts: • Software and its engineering → Automated static analysis; • Theory of computation → Operational semantics; Program analysis; Abstraction; Functional constructs.

Keywords: λ-calculus, control flow analysis, program traces, abstract interpretation, widening

ACM Reference Format:

1 Introduction

Control-flow analysis (CFA) [25, 42] is a family of static analyses whose goal is to determine which functions can be called at a given program point. For this purpose, CFAs generally compute two maps: a cache that determines the closures that each program point may evaluate to, and an environment that describes the values that could be assigned to each variables. With this information, it becomes possible to inline functions, and to remove safely some dynamic tag checks that must be performed in dynamically-typed languages. CFA of higher-order or object-oriented languages is difficult, since the control flow graph of a program is not static. Thus, CFAs try to compute over-approximations of the dynamic call graph. In the functional language community, two main research tracks on CFAs have emerged.

A first group of work has employed constraints to model the conditions under which a solution to a CFA problem is correct. Work in this vein [13, 16, 31, 33, 46] transforms a given program into a logical constraint—usually set-based constraints—that must be solved by a second program—the constraint solver. We refer to this research as “constraint-based analysis” (CBA).

A second group of work has focused on analysing abstract machines, and devised abstract interpretations of (small-step) abstract-machine-based semantics [15, 18, 28, 28]. In this “abstracting abstract machines” (AAM) research track, the low-level elements of abstract machines—environments, stores, continuation stacks—must be abstracted. A related approach has been applied to definitional (big-step) interpreters [4, 9].

The methodology of abstract interpretation [3] has been successfully applied to the AAM approach to justify the soundness of AAM-based analyses. The CBA approach, on the other hand, has focused on syntactic techniques, such as preservation properties, similar to the syntactic type soundness technique. More semantic justifications for the CBA approach, based on abstract interpretation, are still missing.

Although they differ in many ways, the AAM and CBA families have something in common: to ensure the termination of their analyses, they both perform approximations so that their search space becomes finite. Based on the finiteness of the search space, they are able to prove complexity results for CFAs [43]. This finiteness, however, impedes the use of abstract domains with unbounded heights. One such domain is the interval domain, that abstracts sets of integers. The restriction to a finite search space has also diminished the attention to widening techniques [3] for CFAs. While widening is often necessary to ensure the termination of analysers, it is also beneficial in finite domains, where it accelerates the convergence to a solution.

In this paper, we seek to reconcile CFA with abstract interpretation in two ways. First, we show that the control-flow analysis of a λ-term is an abstraction of its execution trace. This trace records two kinds of events: which function calls occurred, and which values were returned at a program point. This suffices to reconstruct the caches and environments found in CFAs. We designed the semantics so that the events track the contexts in which they are produced (at which program point, and after which function call). We
show how to recover the usual notion of call strings [40] from this contextual information. This provides a formalisation of the folklore knowledge that “context-sensitivity is trace partitioning”. This process of building traces and abstracting them is general [2] and can be applied with benefits to other static analyses. Based on this abstraction, we give a modular soundness proof of the constraint-based approach.

In a second stage, we derive by abstract interpretation the VCFA analysis, an expressive control-flow analysis that is built on an infinite domain, and that employs widening to ensure convergence. The precision of this analysis indicates that further research on widening techniques for CFAs is worthwhile.

The contributions of the paper are organised as follows:

- We define a simple, substitution-based small-step semantics for the λ-calculus, that tracks the values produced in each evaluation contexts and the β-reductions that are performed during reduction (§2).
- We define a stack of abstractions (§3) from which we build the global environment and cache found in standard CFAs [33] out of the computation trace of a program. As a methodology, we derive for each abstraction layer the constraints that are satisfied by the abstracted semantics. At the end of our abstraction stack, we obtain a family of CFAs that generalise k-CFA, and that is parameterised by context sensitivity policies.
- Using the previous abstractions, we define a semantic criterion for the solutions of a constraint-based CFA problem. Using this criterion, we give a novel, modular proof of soundness for the constraint rules of k-CFA (§4), where each rule is verified separately. This gives a semantic justification for constraint-based CFA.
- Based on our semantic development, we present VCFA (§5), a novel control-flow analysis that goes beyond the finite state abstraction used in traditional CFAs. VCFA employs a widening operator, that is used at specific points, that are determined by the k⁺ heuristic by limiting call strings to “at most k cyclic call sites”. It can replace the “last k call sites” heuristic from k-CFA.
- Based on the implementation of the analysis, we discuss experimental results (§6), by comparing 0-CFA and 1-CFA with our new analysis and heuristics on a set of example programs taken from the literature. The new analysis takes advantage of non-finite integer domains, such as intervals, to compute more precise approximations with a similar computational cost.

2 A Labelled λ-Calculus

2.1 Syntax

We assume the existence of three infinite sets X, L and P. The set of variables X contains variables, that are denoted by the metavariables x, y, z. The set L contains labels, that are denoted by the metavariable ℓ. Labels are put on lambda abstractions and serve to identify binding sites of variables. The set P contains program points (also called locations), that are denoted by the metavariable p.

Definition 2.1 (Syntax). The set of terms T is inductively defined as follows:

\[ t \in T :\!::=\ x \quad \text{(Variables)} \]
\[ \ell \quad \text{(Abstraction)} \]
\[ tt \quad \text{(Application)} \]
\[ [ ]^n \quad \text{(Annotation)} \]

The terms of the language are the terms of the untyped λ-calculus extended with the annotation construct [t]^n, that has no computational meaning, but is used to collect information about the evaluation of t using the annotation a.

We introduce two kinds of annotations: program points p ∈ P and function calls Call(]\ell x, t, v\]). Program point annotations will serve to record (syntactic) call sites, and function call annotations to keep track of the terms actually applied in the call. Annotation paths π are sequences of annotations, and will serve as contexts. For example, a term \([([\ell x, t, v])^p \text{ reduces to } [[ [x \leftarrow v]] Call(]\ell x, t, v)\]^p\], and any subsequent reduction will happen in a context of the form \(\pi = p \cdot Call(]\ell x, t, v) \cdot \pi'\). This context tells us that the call site of the actual call is p. We let δ range over call site paths i.e. those annotation paths that only consist of program points. We write π₁ · π₂ for the concatenation of paths.

Definition 2.2 (Annotations and paths).

\[ a \triangleq p \quad | \quad \text{Call(}\ell x, t, v\text{)} \quad \text{(Annotations)} \]
\[ \pi \triangleq \varepsilon \quad | \quad \pi a \quad \text{(Annotation paths)} \]
\[ \delta \in \Delta \triangleq \varepsilon \quad | \quad \delta p \quad \text{(Call site paths)} \]

The set of free variables fv t of a term t follows the standard definition. We write t[x ← u] for the term t where the variable x is replaced by the term u (without capture of variables). We omit its definition. The set of values \(\mathbb{V}\) is standard for a call by value λ-calculus.

Definition 2.3 (Values).

\[ v \in \mathbb{V} :\!::=\ \ell x, t \]

2.2 Small-Step Semantics

The small-step semantics is a mostly standard call by value reduction semantics, but extended with events that are emitted at certain reduction steps. A β-reduct is reduced by substituting the actual argument for the formal argument, and by emitting an event \(\beta(\pi, \ell x, t, v)\) signalling that a β-reduction has been performed. Similarly, the reduction of a value under an annotation is done by discarding the annotation and returning the value. This reduction emits an event Ret(\(\pi, a, v\)) recording that the value was returned at that annotation (program point or function call). The path component π of an event will be used to keep track of the execution history that led to the emission of that event—we explain its use in more detail below. The set of traces T is the set of finite
possibly empty) sequences of events. We write \( tr_1 \supseteq tr_2 \) for the concatenation of traces.

**Definition 2.4** (Events and traces),

\[
\mathit{e} \triangleq \mathit{Ret}(\pi, a, v) \quad \mid \quad \mathit{\beta}(\pi, x, t, v) \quad (\text{Events})
\]

\[
\mathit{tr} \in \mathbb{T} \triangleq \varepsilon \quad \mid \quad \mathit{e}, \mathit{tr} \quad (\text{Traces})
\]

The operational semantics uses the following operator for prefixing all events in a trace with an annotation path \( \pi \).

**Definition 2.5** (Prefixing by a path),

\[
\pi \cdot \mathit{Ret}(\pi', a, v) \triangleq \mathit{Ret}(\pi \cdot \pi', a, v)
\]

\[
\pi \cdot \mathit{\beta}(\pi', x, t, v) \triangleq \mathit{\beta}(\pi \cdot \pi', x, t, v)
\]

\[
\pi \cdot \varepsilon \triangleq \varepsilon
\]

\[
\pi \cdot (e, tr) \triangleq (\pi \cdot e), (\pi \cdot tr)
\]

The notation \( e \xrightarrow{c} u \) denotes that the term \( t \) reduces in one step to \( u \), and during this reduction, produces the event \( e \). The definition of the one-step reduction is:

\[
(\lambda x. t) \xrightarrow{\beta(c, x, t, v)} [t[x \leftarrow v]] \text{Call}(\lambda x. t, v)
\]

\[
|v| \xrightarrow{a} \quad v \xrightarrow{c} t' \quad t \xrightarrow{c} t' \quad t \xrightarrow{c} u
\]

As we mentioned earlier, the contraction of a \( \beta_c \)-redex performs a substitution and encloses the redex in an annotation, so as to remember that the reductions that will follow happen in the context of a function call. This is indeed what is meant by the contextual rule for annotations: any event that is emitted under an annotation is reported by prefixing that event with the annotation. Thus, annotations record the contexts of reductions.

The reflexive transitive closure is written \( t \xrightarrow{t} u \), and defined as follows:

\[
|t| \xrightarrow{a} [u]^a
\]

\[
|t| \xrightarrow{c} t_2 \quad |t| \xrightarrow{c} t_3
\]

The rule for reflexivity traces no event, and the rule for transitivity collects the events in the order they occur.

**Lemma 2.6.** The following inference rules are valid:

\[
|t| \xrightarrow{c} u \quad \text{for} \quad t \xrightarrow{t} u
\]

\[
|t| \xrightarrow{c} t_2 \quad |t| \xrightarrow{c} t_3
\]

We give an example of term reduction in Fig. 1. The first step in the evaluation reduces the term annotated with 1 which returns a function. Similarly, the second step evaluates the term annotated with 5 to produce the argument to the function. The third step is the \( \beta \)-reduction that applies the function to the argument, emitting a \( \beta \)-event which states that a \( \beta \)-reduction occurred in the context 0. The two following return steps illustrate how the same lambda term \( \lambda \text{y}. [\text{y}]^6 \) can be returned under different annotations (here, 3 and 4), thereby distinguishing when it is used as a function and as an argument. The context in those two return events is the path \( 0 \cdot C_1 \cdot 2 \) which contains the information that the returned value was obtained by first evaluating the call site annotated with 0, thereby initiating the call \( C_1 \), which in turn led to the call site labelled 2.

**2.3 Trace Collecting Semantics**

We use \( \sigma \) to range over value substitutions, i.e. finite mappings from variables to closed values. The expression \( t \cdot \sigma \) denotes the application of the value substitution \( \sigma \) to the term \( t \) in \( x \) with \( x \) occurrence of \( x \) in \( t \) with \( \sigma(x) \). We write \( \sigma[x \leftarrow v] \) for the substitution \( \sigma \) extended with a new binding that maps \( x \) to \( v \). Given a set of substitutions \( I \), we write \( I[x \leftarrow v] \) for the set \( \{ \sigma[x \leftarrow v] \mid \sigma \in I \} \), and write \( I[x \leftarrow S] \) for the set \( \{ \sigma[x \leftarrow v] \mid \sigma \in I, v \in S \} \).

We consider the following semantics for terms that, given a set of input substitutions, produces a set of pairs, composed of the execution trace and the output value.

**Definition 2.7.** \( |t|_I \triangleq \{ (t, \sigma) \mid t \cdot \sigma \xrightarrow{t} v, \sigma \in I \} \)

**Definition 2.8** (Semantic preorder). We write \( tr_1 \preceq tr_2 \) when \( tr_1 \) is a sub-sequence of \( tr_2 \). It is an order relation. We use the same symbol to denote the following pre-order on sets of traces and values:

\[
S_1 \preceq S_2 \triangleq \forall (t, v), s \in S_1, \exists t^2, t_1 \preceq t^2 \land (t^2, v) \in S_2.
\]

The pre-order \( \preceq \) will serve as the approximation ordering. Larger sets of traces and values are less precise, in the sense that they might contain more traces and output values, and might also contain traces with more events.
Program reduction and trace ordering are related by the following lemma:

**Lemma 2.9 (Preservation).** If \( t_1 \xrightarrow{tr^+} t_2 \), then \( \langle t_2 \rangle_J \leq \langle t_1 \rangle_J \).

The above lemma is central for our semantic framework: it implies that any correct over-approximation of the semantics of \( t_1 \) (in the sense of \( \leq \)) is necessarily a sound approximation of any reduct of \( t_1 \). In other words, the semantic property of being a sound approximation is preserved by reduction. This fact is crucial for the preservation property of CFA constraints from §4 (Lemma 4.2). The proof of Lemma 2.9 is direct: the output values of \( t_1 \) and \( t_2 \) are the same, and the trace produced by \( t_2 \) is a suffix—and thus a sub-sequence—of the trace of \( t_1 \).

In the rest of this paper, we will only consider fully annotated terms as our source language, i.e., terms where variables, applications and abstractions are enclosed in exactly one annotation, which must be a program point. A fully annotated value is an abstraction of a fully annotated term.

For each abstraction that we define in the rest of the paper, we derive the inclusion properties that are satisfied by the abstract semantics. These inclusions naturally lead to the design of analysers in the style of big-step static interpreters [4, 9], that follow the structure of programs.

For fully annotated terms, we get the following inclusions for the trace semantics:

**Lemma 2.10 (Semantic inclusions for annotated terms).**

\[
\begin{align*}
\llbracket x \rrbracket^P_J &= \{ (\text{Ret}(e, p, \sigma(x)), \sigma(x)) \mid \sigma \in I \} \\
\llbracket x.t \rrbracket^P_J &= \{ (\text{Ret}(e, p, \langle x.t \rangle, \sigma), \langle x.t \rangle, \cdot \sigma) \mid \sigma \in I \} \\
\llbracket t_1 \rrbracket^P_J \cdot \llbracket t_2 \rrbracket^P_J \leq & (p \cdot t_1 + p \cdot \tilde{t}_2 + \\
& \beta(p, \langle x \rangle \cdot \langle t_1 \rangle, \langle t_2 \rangle, v_2) + \\
& p \cdot \text{Call}(\langle x \rangle \cdot \langle t_1 \rangle, \langle t_2 \rangle) \\
& \text{Ret}(p, \text{Call}(\langle x \rangle \cdot \langle t_1 \rangle, \langle t_2 \rangle, v_2), v_3) \\
& + \text{Ret}(e, p, v_3, v_1) \}
\end{align*}
\]

For variables, the semantics produces return events only, where the returned values are read in the possible input substitutions. The case for functions is similar: the returned values are functions whose free variables are substituted for the values given by the input variables.

In the inclusion for fully annotated applications, the execution trace \( \tilde{t}_3 \) that corresponds to the function call is enclosed in the following two events: the event \( \beta(p, \langle x \rangle \cdot \langle t_1 \rangle, \langle t_2 \rangle, v_2) \) that denotes the start of the function call, and the event \( \text{Ret}(p, \text{Call}(\langle x \rangle \cdot \langle t_1 \rangle, \langle t_2 \rangle, v_2), v_3) \), that denotes the return from that function call. Interestingly, the same trace \( \tilde{t}_3 \) is prefixed with the location \( p \cdot \text{Call}(\langle x \rangle \cdot \langle t_1 \rangle, \langle t_2 \rangle) \), that records which function call is considered, and where it happened. In usual CFA analyses for functional languages, only the \( \text{locus} \ p \) of the function call is remembered.

\[T \rightarrow R(\text{Clos}) \times (X \xrightarrow{\text{fin}} (L \times D)) \rightarrow R(\text{Clos}) \times C(\text{Clos})\]
\[\gamma_\phi \downarrow \alpha_\phi \text{ context projection (§1.7)}\]
\[T \rightarrow R(\text{Clos}) \times (X \xrightarrow{\text{fin}} (L \times D)) \rightarrow R(\text{Clos}) \times C(\text{Clos})\]
\[\gamma_\text{Clos} \downarrow \text{induction abstraction (§1.6)}\]
\[T \rightarrow \varphi(X \xrightarrow{\text{fin}} \text{V}) \rightarrow R(\text{V}) \times C(\text{V})\]
\[\gamma_M \downarrow \alpha_M \text{ independent attribute for inputs (§1.4)}\]
\[T \rightarrow \varphi(X \xrightarrow{\text{fin}} \text{V}) \rightarrow R(\text{V}) \times C(\text{V})\]
\[\gamma_{\text{Clos}} \downarrow \alpha_{\text{Clos}} \text{ independent attribute for inputs (§1.3)}\]
\[T \rightarrow \varphi(X \xrightarrow{\text{fin}} \text{V}) \rightarrow R(\text{V}) \times C(\text{V})\]
\[\gamma_{\text{NoVal}} \downarrow \alpha_{\text{NoVal}} \text{ independent attribute for pairs (§1.3)}\]
\[T \rightarrow \varphi(X \xrightarrow{\text{fin}} \text{V}) \rightarrow R(\text{V}) \times C(\text{V}) \times V\]
\[\gamma_h \downarrow \alpha_h \text{ history obligation (§1.2)}\]
\[T \rightarrow \varphi(X \xrightarrow{\text{fin}} \text{V}) \rightarrow R(\text{V}) \times C(\text{V}) \times V\]
\[\gamma_e \downarrow \alpha_e \text{ event selection (§1.1)}\]

**Figure 2. Abstraction steps.**

3 A Systematic Reconstruction of CFA

Standard control flow analyses for a program \( t \) construct two objects as results of the analysis. The first object is a global environment \( \hat{\beta} \) that records the set of values that variables of \( t \) could have been assigned to. To distinguish between several instances of variables, variables are distinguished by their calling context—sometimes also called memento [31, 33] or instances [37]. A global environment maps a pair \((x, \delta)\) of a variable and its calling context to a set of abstract values. The global environment is called global store in the AAM line of work. In this paper, instead of taking variables and contexts \((x, \delta)\) as keys of global environments, we choose binding sites (corresponding to \( \lambda \)-abstractions) and contexts \((t, \delta)\) as keys. This choice is technical and can be ignored in a first read: it ensures that our definitions do not depend on the names of variables, and are consistent with the \( \alpha \)-equivalence of \( \lambda \)-terms. We write \( R(A) \triangleq (L \times D) \rightarrow \varphi(A) \) for the type of global environments that contain sets of elements of type \( A \).

The second object computed by a CFA is a global cache \( \mathcal{C} \), that maps every sub-term of the program \( t \)—identified by their program points—to a set of abstract values that denotes the possible evaluation results of that sub-term. Similarly
to global environments, different versions of sub-terms are distinguished by their evaluation contexts. A global cache therefore maps a pair \((p, \delta)\) of a program point and an evaluation context to a set of abstract values. Some analyses remove the need of a cache by working with administrative normal forms (ANF), where every sub-term is bound to a variable. We write \(C(A) \equiv (\mathbb{P} \times \mathbb{D}) \rightarrow \varphi(A)\) for the type of global caches that contain sets of elements of type \(A\).

In this section, we show how to reconstruct the environments and caches of \(k\)-CFA as abstractions of the trace-based semantics. The abstraction strategy is summarised in Fig. 2. Most abstractions form Galois connections [3]. A Galois connection between partially ordered sets is defined as follows:

**Definition 3.1 (Galois connection).** We write \((A, \leq_A) \xrightarrow{\gamma} (B, \leq_B)\) when for any \(a \in A\) and \(b \in B\), \(a \leq_A b \iff a \leq_A \gamma(b)\).

The first stages of abstraction—starting from the bottom of Fig. 2—are responsible for selecting events in the traces, and forgetting about the ordering of events. After these preliminary steps, we have built environments and caches of types \(\mathbb{R}(V)\) and \(C(V)\), that contain sets of values. Then, inputs are abstracted and finally values are abstracted by the closure abstraction and the indirection abstraction. These two abstractions are not Galois connections, as there is no best way to perform these abstractions, but they still lead to correct analyses.

The closure abstraction builds abstract closures, composed of some code and some environment, that maps variables to sets of abstract closures. Then, the indirection abstraction introduces intermediate names of type \(\mathbb{L} \times \mathbb{D}\): at this level, abstract closures are composed of some code together with an environment that maps variables to names. This indirection is similar to the indirection used in the small-step semantics of the AAM line of work, where names are called *addresses*.

Finally, the last abstraction step modifies the calling contexts in names using a projection function \(\phi\): we recover \(k\)-CFA by choosing \(\phi(\delta) = [\delta]_k\), that is the truncation to the last \(k\) elements of \(\delta\).

In the following subsections, we define the abstractions of the semantics and, at some key steps, show how they impact the semantic inclusions. We exploit those inclusions in §4 to semantically justify the constraints of \(k\)-CFA.

### 3.1 Abstraction of Events

We select events by performing two transformations on traces. First, we select the *call sites* in the contexts of events. The call sites are the program points that occur just before a \(\text{Call}(v_1, v_2)\) annotation. Recall the example from §2.1 with \([\langle X, t \rangle \cdot v]\) that reduces to \([\langle t[x \leftarrow v] \rangle^{\text{call}(\langle X, t \rangle \cdot v)}]\). Subsequent reductions will happen in a context of the form \(\pi = p \cdot \text{Call}(\langle X, t \rangle \cdot v) \cdot \pi'\), recording that the call site of the actual call is \(p\). Thus, to recover the standard call site information we just need to keep the information \(\text{calls}(\pi) = p \cdot \text{calls}(\pi')\).

The call filtering is extended to events and traces as follows:

**Definition 3.2 (Call filtering).**

- On paths: \(\text{calls} \epsilon \triangleq \text{calls}(a \cdot \epsilon) \triangleq \epsilon\)
- \(\text{calls}(p \cdot \text{Call}(v_1, v_2) \cdot \pi) \triangleq p \cdot \text{calls} \pi\)
- \(\text{calls}(p_1 \cdot p_2 \cdot \pi) \triangleq \text{calls}(p_2 \cdot \pi)\)

- On events:
  - \(\text{calls}(\text{Ret}(\pi, a, v)) \triangleq \text{calls}(\pi, a, v)\)
  - \(\text{calls}(\beta(\pi, v_1, v_2)) \triangleq \beta(\text{calls}(\pi, v_1, v_2))\)

- On traces:
  - \(\text{calls} \epsilon \triangleq \epsilon\)
  - \(\text{calls}(e, \text{tr}) \triangleq (\text{calls} e, (\text{calls} tr))\)

We deliberately drop the Call annotations, because our goal is to recover eventually the *call strings* that are used in \(k\)-CFA. We leave to future work the question of keeping Call annotations to obtain other forms of context sensitivity.

The second selection pass on events consists in keeping only events that are labelled by program points—as opposed to call annotations. This is simply done as follows:

**Definition 3.3 (Event filtering).**

\[
\begin{align*}
\text{ret} \epsilon & \triangleq \epsilon \\
\text{ret}(\beta(\pi, v_1, v_2), \text{tr}) & \triangleq \beta(\pi, v_1, v_2), \text{ret} \text{tr} \\
\text{ret}(\text{Ret}(\pi, a, v), \text{tr}) & \triangleq \text{Ret}(\pi, a, v), \text{ret} \text{tr} \\
\text{ret}(\text{Ret}(\pi, \text{Call}(v_1, v_2), a), \text{tr}) & \triangleq \text{ret} \text{tr}
\end{align*}
\]

By composing the two filter functions, we obtain the abstraction function \(\alpha_e\) for events, together with its corresponding concretization \(\gamma_e\):

**Definition 3.4 (Event abstraction and concretization).**

\[
\alpha_e(S) \triangleq \{(\text{ret} \circ \text{calls}(\text{tr}), v) \mid (\text{tr}, v) \in S\}
\]

\[
\gamma_e(S) \triangleq \{(\text{tr}, v) \mid \text{ret} \circ \text{calls}(\text{tr}) \leq \text{tr'} \land (\text{tr'}, v) \in S\}
\]

**Lemma 3.5.** The functions \(\alpha_e\) and \(\gamma_e\) form a Galois connection: \((\phi(T \times \forall), \leq) \xrightarrow{\gamma_e} (\phi(T \times \forall), \leq)\).

The proof relies on the monotonicity of calls and ret with respect to the sub-sequence order.

The function \(\alpha_e(t[I])\) for a fully annotated term \(t\) satisfies the following inclusions:

**Lemma 3.6 (Semantic inclusions after event abstraction).**

\[\alpha_e([x]_I]_T) = \{(\text{Ret} e, p, \sigma(x)), \sigma(x) \mid e \in I\}\]

\[\alpha_e([\langle X, t \rangle]_T]_I = \{(\text{Ret}(e, p, \langle X, t \cdot \sigma \rangle), \langle X, t \cdot \sigma \rangle) \mid e \in I\}\]

\[\alpha_e([[t_1]_I]^{[t_2]_I]_T) \leq \begin{cases} 
(\text{tr}_1 + \text{tr}_2) + & (\text{tr}_1, \langle X, t_1 \rangle, t_2) \in \alpha_e([t_1]_I) \\
(\beta(p, \langle X, t_1 \rangle) \cdot v_2) + & \text{and } (\text{tr}_2, v_2) \in \alpha_e([t_2]_I) \\
p \cdot \text{tr}_3 + \text{Ret}(e, p, v_3), & \text{and } (\text{tr}_3, v_3) \in \alpha_e([t_3]_I) \\
& \text{and } (\text{tr}_3, v_3) \leq \alpha_e([t_3]_I)\}
\end{cases}\]

Compared to Lemma 2.10, we notice that the events and contexts involved in a call annotation have been removed. In particular, the trace \(\text{tr}_1\) that corresponds to the evaluation of the function body obtained from \(t_1\) is now only prefixed by the call site \(p\), i.e. the program point of the application.

### 3.2 Unordered History Abstraction

In this abstraction step, we forget the order of events in the computation trace. Instead of a trace, we produce two maps that contain sets of values.
The first map is a global environment that inspects the $\beta$-reduction events and remembers on which arguments the functions were called, and in which context. This environment map is defined by the env function.

The second map is a global cache, that reads the return events and remembers which values were produced for the different program points, and in which context. This cache map is defined by the cache function.

**Definition 3.7** (Building environments and caches).

$$
\text{env}(e) \triangleq \emptyset
$$

$$
\text{env}(\text{Ret}(\delta, p, o), tr) \triangleq \text{env} \ tr
$$

$$
\text{env}(\beta(\delta, x, t, o), tr) \triangleq \{(t, \delta) \mapsto \{v\} + \text{env} \ tr
$$

$$
\text{cache}(e) \triangleq \emptyset
$$

$$
\text{cache}(\text{Ret}(\delta, p, o), tr) \triangleq \{(p, \delta) \mapsto \{v\} + \text{cache} \ tr
$$

$$
\text{cache}(\beta(\delta, x, t, o), tr) \triangleq \text{cache} \ tr
$$

The definitions of env and cache rely on the following operations on maps with a set-valued range.

**Definition 3.8** (Operations and relations on maps).

$$
\emptyset \triangleq \lambda k.k.\emptyset
$$

$$
\emptyset \triangleq \lambda k. k'
$$

$$
\{k \mapsto S\} \triangleq \lambda k. k'
$$

$$
\{k \mapsto S\} \triangleq \{k \mapsto S\}
$$

$$
\pi \cdot m \triangleq \lambda (x, \pi'). \text{if } \pi' = \pi \cdot \pi'' \text{ then } m(\pi'') \text{ else } \emptyset
$$

$$
m_1 + m_2 \triangleq \lambda k. m_1(k) \cup m_2(k)
$$

$$
m_1 \subseteq m_2 \triangleq \forall k. m_1(k) \subseteq m_2(k)
$$

The above definitions comprise the empty map, the singleton map, how to preform a map with a path, how to take the union of two maps, and how to compare them. The definitions of history abstraction and concretization follow.

**Definition 3.9** (History abstraction and concretization).

$$
a_h(S) \triangleq \{(\text{env} \ tr, \text{cache} \ tr, o) \mid \text{tr}, o \in S\}
$$

$$
\gamma_h(S) \triangleq \{(\text{tr}, o) \mid \text{env} \ tr \subseteq \rho \land \text{cache} \ tr \subseteq C \land (\rho, C, o) \in S\}
$$

$$
\delta_1 \subseteq \delta_2 \triangleq \forall (\rho, C_1, o_1) \in \delta_1. \exists (\rho_2, C_2, o_2) \in \delta_2.

\rho_1 \subseteq \rho_2 \land C_1 \subseteq C_2 \land o_1 = o_2
$$

**Lemma 3.10.** ($\varphi(\sum, \times, \vee) \subseteq \prod_{\text{env}} (\varphi(\mathbb{R}(\mathbb{V})) \times C(\mathbb{V}) \times \mathbb{V}), \emptyset)\n
The proof relies on the monotonicity of env and cache.

We write $a_h = a_0 \circ a_c$ for the chaining of the abstractions we have defined so far. The abstract semantics of a fully annotated term $A_h([t])_I$ satisfies the following inclusions:

**Lemma 3.11** (Semantic inclusions after history abstraction).

$$
A_h([x]_I^p) = \{((\emptyset, \{(p, e) \mapsto \{\sigma(x)\}, \sigma(x) \mid \sigma \in I\}
$$

$$
A_h([x.x]_I^p) = \{((\emptyset, \{(p, e) \mapsto \{v\}, o) \mid o = (x.x) \cdot \sigma, \sigma \in I\}
$$

$$
A_h([x]_I^p \cdot [t]_I^p) = \{(p_1 + p_2 + p \cdot C_1 + p_3, C_3, \sigma, \sigma \in I\}
$$

$$
\{((t, p) \mapsto \{v_2\})
$$

The call site $p$ prefixes the environment $p_1$ and cache $C_3$ that result from the evaluation of the function body of the application. Moreover, the global environment records that the arguments of these functions contain the possible values for the arguments of the application. Finally, the global cache remembers that the whole term, i.e. the program point $p$ in the empty environment, evaluates to the possible values of the function body.

### 3.3 Forgetting Output Values and Creation of Environments and Caches

The next abstraction steps are administrative, simple, and use mostly standard Galois connections. We only give a brief sketch of how they work.

First, we only keep the environment and the cache, using the abstraction function $\alpha_{\text{env}}(S) \triangleq \{(\rho, C) \mid \exists o. (\rho, C, o) \in S\}$. Then, we separate environments from caches: using the function $\alpha_X(S) \triangleq \{(\rho \mid \exists C, (\rho, C, o) \in S), (\rho \mid \exists o, (\rho, C, o) \in S)\}$, we transform sets of pairs of maps into sets of maps. Finally each set of environments or caches—is abstracted as a map—an environment or a cache, respectively—using the function $\alpha_{\text{env}}(S) \triangleq \lambda k. \bigcup_{m \in \mathbb{M}} m(k)$ to abstract the maps, and $\alpha_X(S_1, S_2) \triangleq (\alpha_X(S_1), \alpha_X(S_2))$ to abstract their pairs. All these functions are adjoints of Galois connections.

We define the function $A_{\text{EC}} \triangleq a_{\text{env}} \circ a_X \circ a_{\text{env}} \circ a_h$, that stacks up all the abstractions we have defined so far. The semantic inclusions for the abstract semantics of a fully annotated term $A_{\text{EC}}([t]_I^p)$ are easily obtained, by noticing that for a term $[t]_I^p$ with an output value $v$ and a cache $C$ obtained by $A_h([t]_I^p)_I$, we always have $\{v\} \subseteq C(p, e)$.

### 3.4 Abstracting Inputs

The next abstraction abstracts the set of inputs $I$. We transform this set of substitutes—i.e. maps from variables to values—into a map from variables to sets of values, using the Galois connection $\Rightarrow_{\mathbb{M}_I}$ we defined in the previous section. We denote by $E$ the maps from variables to sets of values. The abstract semantics $A_{\text{EC}}([t]_I^p)_{\mathbb{M}(E)}$ of a fully annotated term $[t]_I^p$ satisfies the following inclusions:

**Lemma 3.12** (Semantic inclusions after input abstraction).

$$
A_{\text{EC}}([x]_I^p)_{\mathbb{M}(E)} \subseteq \{(\emptyset, \{(p, e) \mapsto (x)\})
$$

$$
A_{\text{EC}}([x.x]_I^p)_{\mathbb{M}(E)} = (\emptyset, \{(p, e) \mapsto \{(x.x) \cdot \sigma \mid \sigma \in \mathbb{M}(E)\})
$$

$$
A_{\text{EC}}([x]_I^p \cdot [t]_I^p)_{\mathbb{M}(E)} \subseteq \{(p_1 + p_2 + p_3, C_1 + C_2 + C_3, \sigma_1, \sigma_2 \in I)\}
$$

where $(p_1, C_1) = A_{\text{EC}}([t]_I^p)_{\mathbb{M}(E)}$ and $(p_2, C_2) = A_{\text{EC}}([t]_I^p)_{\mathbb{M}(E)}$. 

$$
p_3 = \sum \delta_{x, t} \cdot \rho_{\text{EC}} \cdot \mathbb{P} \cdot \text{fst} \cdot A_{\text{EC}}([t]_I^p)_{\mathbb{M}(x \mapsto C_2(p_1, e))}
$$

$$
+ \{(t, p) \mapsto C_2(p_2, e)\}
$$

$$
C_3 = \sum \delta_{x, t} \cdot \rho_{\text{EC}} \cdot C_2
$$

$$
\text{let } C_3' = \text{snd} \cdot A_{\text{EC}}([t]_I^p)_{\mathbb{M}(x \mapsto C_2(p_1, e))} \text{ in } p \cdot C_3' + \{(t, p) \mapsto C_3(p_3, e)\}
$$

In the case of variables, the cache is built by reading the set of possible values in the environment.

For $\lambda$-abstractions, the cache uses the set of values that results from closing the $\lambda$-abstraction being analysed under all the possible substitutions that belong to the concretized
3.5 Closure Abstraction

In this abstraction step, we introduce an abstract domain to represent sets of closures. An abstract closure is composed of a value—a λ-abstraction—and an environment that assigns to each of the free variables of the value a set of abstract closures. The definition of this abstract domain is recursive. This abstract domain will be the starting point of the new analysis VCFWA as defined in §5.

Definition 3.13 (Abstract closures and their concretization).

\[
\begin{align*}
\text{Clos} & \triangleq \forall \times \mathcal{G} \\
\mathcal{G} & \triangleq X \xrightarrow{\text{fn}} \wp(\text{Clos}) \\
\gamma_0 & \triangleq \forall \mathcal{M} \circ \gamma_{\text{clo}} \\
\gamma'_{\text{clo}}(S) & \triangleq \bigcup_{t, x} \{ (t, x) \sigma | \sigma \in \gamma_0(t) \}
\end{align*}
\]

The concretization of a set of closures builds the set of values for each closure in the set by closing over all the possible environments, and then takes the union of those sets. The inclusions for the abstracted semantics follow:

Lemma 3.14 (Semantic inclusions after closure abstraction).

\[
\begin{align*}
A_{\text{EC}}([t_1]p_1)^{\gamma_0}(\mathcal{G}) & \triangleq 2\gamma_{\text{clo}}(\emptyset, \{ (p, \epsilon) \mapsto (t_1) \}) \\
A_{\text{EC}}([\lambda x.x][t_1]p_1)^{\gamma_0}(\mathcal{G}) & \triangleq 2\gamma_{\text{clo}}(\emptyset, \{ (p, \epsilon) \mapsto \{ (t, x) \mathcal{G} | \mathcal{G} \in \gamma_0(t) \} \})
\end{align*}
\]

\[
\begin{align*}
A_{\text{EC}}(([t_1]p_1)[t_2]p_2)^{\gamma_0}(\mathcal{G}) & \triangleq 2\gamma_{\text{clo}}(\emptyset, \{ (p, \epsilon) \mapsto \{ (t, x) \mathcal{G} | \mathcal{G} \in \gamma_0(t) \} \})
\end{align*}
\]

and

\[
\begin{align*}
A_{\text{EC}}([t_1][t_2]p_2)^{\gamma_0}(\mathcal{G}) & \triangleq 2\gamma_{\text{clo}}(p_2, C_2)
\end{align*}
\]

There are two main differences compared to the inclusions of Lemma 3.12. First, in the case of λ-abstractions, an abstract closure is now built, using the input environment to form the closure. Second, in the case of applications, we obtain abstract closures \(\lambda x.t_1\)[[t_2]][t_1] by analysing \([t_1][t_2]p_2\). The bodies \([t_1][t_2]\) of these closures are then analysed in the environment \(\mathcal{G}_1\) extended by mapping \(x\) to the values from \(C_2(p_2, \epsilon)\), i.e. the possible values of the argument \(t_2\).

3.6 Indirection Abstraction

The indirection abstraction is the most complex of this paper, and constitutes a crucial step to eventually recover the textbook definition of k-CFA. The idea of the abstraction is to introduce an indirection through names to break the recursion cycle in the definition of closures. Here, we choose call strings as names. Previous work from the AAM family has developed this idea too, also to break circularity. They baked the indirection in their semantics using a global store.

The new abstract closures \(\hat{c} \in \hat{\text{Clos}}\) are composed of a λ-abstraction and an environment \(\hat{\mathcal{G}} \in \hat{\mathcal{G}}\) that assigns to each free variable a binding label \(\ell\) and a name \(\delta\) as opposed to a set of closures as done in §3.5. The binding label refers to the binding site of the variable, and the name \(\delta\) refers to the context in which the variable has been assigned to a value.

Definition 3.15 (Indirection abstraction).

\[
\begin{align*}
\hat{\text{Clos}} & \triangleq \forall \times \hat{\mathcal{G}} \\
\hat{\mathcal{G}} & \triangleq \mathbb{X} \xrightarrow{\text{fn}} (\mathbb{L} \times \mathbb{D})
\end{align*}
\]

\[
\begin{align*}
\langle t, x, \ell \rangle & \in \hat{\text{Clos}} \iff \exists \hat{\ell}, \langle t, x, \ell \rangle \in S \land \Gamma = \text{dom} \hat{\mathcal{G}} \\
\forall x \in \text{dom} \hat{\mathcal{G}}, \forall \mathcal{V} \in \Gamma(x), c \in \gamma_{\text{ind}}(\hat{\mathcal{G}}(x))
\end{align*}
\]

\[
\begin{align*}
\gamma_{\text{ind}}(\hat{c}) & \triangleq \{ c | c \in \gamma_{\text{ind}}(\hat{c}) \} \\
\gamma_{\text{ind}}(m) & \triangleq \text{map}_{\text{ind}}(\hat{c}, m)
\end{align*}
\]

\[
\begin{align*}
\gamma_{\text{clm}} & \triangleq \gamma_{\text{clo}} \circ \gamma_{\text{ind}} \circ \gamma_{\text{clm}}(\hat{\mathcal{G}})
\end{align*}
\]

The meaning of an abstract closure depends on a global environment \(\hat{\rho} \in \mathbb{R}(\hat{\text{Clos}})\), that maps pairs \((\ell, \delta)\) to sets of abstract closures with indirection. An abstract closure with indirection denotes the set of the abstract closures that are obtained by unfolding the definitions contained in \(\hat{\rho}\) a finite number of times. We formally define this in Def. 3.15, using the inductively defined relation \(\in_{\text{ind}}\) that performs these unfoldings. Our concretization function \(\gamma_{\text{ind}}^-1\) transforms a set of abstract closures in \(\hat{\text{Clos}}\) into a set of abstract closures in \(\text{Clos}\) from §3.5. Our definitions are inspired from the correctness relation \(R\) of [33, p. 159]—an inductive relation that describes the concrete closures that are obtained by finitely unfolding indirections.

The semantic inclusions that result from the indirection abstraction are similar to those of Lemma 3.14.

Lemma 3.16 (Inclusions after indirection abstraction).

\[
\begin{align*}
A_{\text{EC}}([[x]p_1]^{\gamma_0}(\hat{\mathcal{G}})) & \triangleq 2\gamma_{\text{clm}}(\emptyset, \{ (p, \epsilon) \mapsto \hat{\rho}(\hat{\mathcal{G}}(x)) \})
\end{align*}
\]

\[
\begin{align*}
A_{\text{EC}}([[t]p_1][t_2]p_2)^{\gamma_0}(\hat{\mathcal{G}}) & \triangleq 2\gamma_{\text{clm}}(\hat{\rho}, \hat{\mathcal{G}}(x) \mapsto \{ (t, x) \mathcal{G} | \mathcal{G} \in \gamma_{\text{ind}}(\hat{\mathcal{G}}(x)) \})
\end{align*}
\]

\[
\begin{align*}
A_{\text{EC}}([t_1][t_2]p_2)^{\gamma_0}(\hat{\mathcal{G}}) & \triangleq 2\gamma_{\text{clm}}(\hat{\rho}_{\text{ind}}(\hat{\mathcal{G}}(x)), \hat{\mathcal{G}}(x))
\end{align*}
\]

and

\[
\begin{align*}
A_{\text{EC}}([t_1][t_2]p_2)^{\gamma_0}(\hat{\mathcal{G}}) & \triangleq 2\gamma_{\text{clm}}(\hat{\rho}_{\text{clm}}(\hat{\mathcal{G}}(x)), \hat{\mathcal{G}}(x))
\end{align*}
\]
The semantic inclusions exhibit one degree of freedom, in the case of applications. The name $\delta(\ell)$ to assign to the arguments of function bodies can be chosen freely, as long as the global environment satisfies that the possible values for the argument in the context $\delta(\ell)$ contains the possible values of $t_2$. This degree of freedom has been thoroughly explored by the AAM line of work, through the use of specific allocation functions. In CFA, the standard choice is to take the current enclosing context extended with $p$ (the call site).

In §4, we will exploit the inclusions of Lemma 3.16 to justify the constraint rules for \(\infty\)-CFA.

### 3.7 Call Sites Abstraction: Context Projection

The final abstraction step is to lose information by identifying certain contexts. This is where standard CFAs transform the search space into a finite one. We model this collapse of the search space by a projection function $\phi \in \mathcal{D} \rightarrow \mathcal{D}$.

**Definition 3.17** (Context projection abstraction)

$\alpha_D(\phi)(m) \triangleq \lambda(x, \delta). \bigcup \{\delta'(x, \delta') \mid m(x, \delta')\}$

$\gamma_D(\phi)(m) \triangleq \lambda(x, \delta). m(x, \phi(\delta))$

The action of $\phi$ on maps is to unite the sets that are assigned to the keys $k_1$ and $k_2$, when $\phi(k_1) = \phi(k_2)$. So far, no hypothesis on $\phi$ is required. The functions $\phi$ define the context sensitivity policies of the analysis. By taking $\phi(\delta) = \delta$, we keep the same abstract semantics, i.e., \(\infty\)-CFA. If we take $\phi(\delta) = \epsilon$, there is no distinction between contexts anymore, and we obtain 0-CFA. To get $k$-CFA, we take $\phi(\delta) = [\delta]_k$, i.e. the function that keeps the last $k$ elements of $\delta$.

**Lemma 3.18.** $\alpha_D(\phi)$ and $\gamma_D(\phi)$ form a Galois connection: $(\mathbb{R}(\text{Clos}) \times \mathbb{C}(\text{Clos}), \leq)$ $\Leftrightarrow (\mathbb{R}(\text{Clos}) \times \mathbb{C}(\text{Clos}), \leq_\phi)$

### 4 Constraint-Based CFA

As a first illustration of the use of the abstractions defined in the previous sections, we show how they enable a semantic and modular soundness proof of the constraint rules for infinitary CFA—where no approximation of contexts is performed—and for $\phi$-CFA, a family of analyses parameterised by a projection function $\phi$, that generalises uniform $k$-CFA. More specifically, we give a semantic definition of what it means for a pair $(\hat{\rho}, \hat{\mathcal{C}})$ to be a solution of a CFA problem.

As a consequence, the syntactic constraint rules become theorems. A benefit of this approach is that the proof method is modular: each rule is proved sound separately, instead of considering the set of rules as a whole.

We use the same notation $(\hat{\rho}, \hat{\mathcal{C}}) \models_D [t]^p$ as in [33, p. 190], that defines the valid solutions of a CFA problem. This judgement denotes that $(\hat{\rho}, \hat{\mathcal{C}})$ is a valid solution for the CFA of the term $[t]^p$, taken in the calling context $\delta$ and in the environment $\hat{\Gamma}$. Our semantic definition follows:

**Definition 4.1** (Semantic validity of an $\infty$-CFA solution).

$(\hat{\rho}, \hat{\mathcal{C}}) \models_D [t]^p \triangleq \delta \cdot A_{\text{EC}}([t]^p)_{\hat{\rho}} \models_{\text{EC}} \gamma_{\text{Clos}} \circ \gamma_{\text{Ind}} \circ \hat{\mathcal{C}}$  

The validity of the solution $(\hat{\rho}, \hat{\mathcal{C}})$ is stated as an overapproximation property. Consider the set of inputs $I$ defined by $\hat{\Gamma}$ under the definitions of $\hat{\rho}$, i.e., $I = \gamma_{\text{EC}}(\hat{\rho}, \hat{\Gamma})$. The definition tells us that $(\hat{\rho}, \hat{\mathcal{C}})$ must be an over-approximation of the semantics of the program $[t]^p$ for the set of inputs $I$, where this semantics is considered “in the calling context $\delta$.” This is why the maps obtained by abstracting the semantics are prefixed with the call site path $\delta$.

From Lemma 2.9 and the monotonicity of the abstractions it follows that semantic validity is preserved by reduction:

**Lemma 4.2.** If $t_1 \xrightarrow{\tau^*} t_2$ and $(\hat{\rho}, \hat{\mathcal{C}}) \models_D t_1$, then $(\hat{\rho}, \hat{\mathcal{C}}) \models_D t_2$.

The proof method we employ for the preservation property radically differs from previous proofs used in constraint-based approaches [16, 17, 33, 46], where preservation is proved in a syntactic manner, by reasoning globally on the whole set of rules that define the constraints: their proofs inspect complete derivation trees built from the rules for the initial program, and reconstruct derivation trees for the reduced program. Such proofs follow the style of subject reduction proofs for type systems [35], and are hard to maintain and to extend. In contrast, our proof of preservation is short and simple, and is independent of the set of rules, as it relies only on the definition of semantic validity and on the monotonicity of the abstractions.

Our central result is the following theorem, that asserts the soundness of the rules for \(\infty\)-CFA.

**Theorem 4.3** (Constraints for \(\infty\)-CFA). The following inference rules are sound:

$(\hat{\rho}, \hat{\mathcal{C}}) \models_{\text{EC}} [x]^p$ 

$(\hat{\rho}, \hat{\mathcal{C}}) \models_{\text{EC}} [x,y]^p$ 

$(\hat{\rho}, \hat{\mathcal{C}}) \models_{\text{EC}} [x_1,x_2]^p$ 

$(\hat{\rho}, \hat{\mathcal{C}}) \models_{\text{EC}} [x_1,x_2]^p$ 

$(\hat{\rho}, \hat{\mathcal{C}}) \models_{\text{EC}} [x_1,x_2]^p$ 

$(\hat{\rho}, \hat{\mathcal{C}}) \models_{\text{EC}} [x_1,x_2]^p$ 

$(\hat{\rho}, \hat{\mathcal{C}}) \models_{\text{EC}} [x_1,x_2]^p$ 

$(\hat{\rho}, \hat{\mathcal{C}}) \models_{\text{EC}} [x_1,x_2]^p$ 

$(\hat{\rho}, \hat{\mathcal{C}}) \models_{\text{EC}} [x_1,x_2]^p$ 

$(\hat{\rho}, \hat{\mathcal{C}}) \models_{\text{EC}} [x_1,x_2]^p$ 

The proof relies on the inclusions provided by Lemma 3.16. The main arguments to conduct the proof are the monotonicity of the path-prefixing operator, and the fact that both path-prefixing and map-union semi-commute with the concretisations $\gamma_{\text{Clos}}$ and $\gamma_{\text{Ind}}$ (i.e., $\delta \cdot \gamma(m) \leq \gamma(\delta \cdot m)$ and $\gamma(m_1) + \gamma(m_2) \leq \gamma(m_1 + m_2)$ for the order relations of interest). Importantly, each rule is proved sound independently of each other. We believe this makes sound control-flow analyses easier to design, and also more robust to extend with new features. To our knowledge, this is the first compositional explanation of a context-sensitive CFA.

By proceeding in a similar way as for \(\infty\)-CFA, we can generalise the previous results to the validity of $\phi$-CFA, i.e. a CFA problem where the calling contexts are projected by
a function $\phi$. The statement differs from Def. 4.1 only by adding a call to the abstraction function $\alpha_\mathcal{O}(\phi)$ from §3.6.

**Definition 4.4** (Semantic validity of a $\phi$-CFA solution). $(\phi, \hat{\rho}, \hat{C}) \models [t]^p \triangleq \alpha_\mathcal{O}(\phi)(\delta \cdot \Delta_E\{[t]^p\}_{\gamma_0(\hat{\rho}, \hat{C})}) \leq \hat{C}_{\text{clos}} \circ \gamma_{\text{cl}}(\hat{\rho}, \hat{C})$

The following theorem follows. If we take $\phi(\delta) = [\delta]_k$, the theorem gives a semantic justification for the textbook constraint rules of uniform $k$-CFA.

**Theorem 4.5** (Constraints for $\phi$-CFA). Assume that $\phi \circ \phi = \phi$ and that $\delta$ and every path that occurs in $\hat{\rho}, \hat{C}, \hat{F}$ are fixpoints of $\phi$. Then, the following inference rules are sound:

- $(\hat{\rho}, \hat{C}) \models [t]^p \triangleq \alpha_\mathcal{O}(\phi)(\delta) \cdot \Delta_E\{[t]^p\}_{\gamma_0(\hat{\rho}, \hat{C})}) \leq \hat{C}_{\text{clos}} \circ \gamma_{\text{cl}}(\hat{\rho}, \hat{C})$

As expected, the rules differ from those of $\infty$-CFA only in the application rule, where the projection $\phi$ is used to project the extended calling context $\delta p$ during the analysis of the function bodies. The idempotency hypothesis $\phi \circ \phi = \phi$ ensures that the new paths $\phi(\delta p)$ are fixpoints of $\phi$, which is made necessary by our requirement that $\hat{\rho}$ and $\hat{C}$ should only contain paths that are fixpoints of $\phi$.

In $k$-CFA, the chosen $\phi$ is such that $\phi$ has a finite range. This ensures that there is a finite number of $\Gamma$, $\hat{\rho}$ and $\hat{C}$. Consequently, the resolution of the system of constraints necessarily explores a finite number of states, because the set of states has been made finite. In §5, we consider instead a system where the set of states is infinite, but where the algorithm is guaranteed to explore a finite number of them. This is achieved by widening techniques.

To conclude this section, we give the precise semantic property that a solution to $\phi$-CFA enjoys.

**Theorem 4.6.** Assume $(\phi, \hat{\rho}, \hat{C}) \models [t_0]^p$ and $[t_0]^p \rightarrow v_0$ and $t_0$ is a closed program. Then:

- If $\beta(\pi, X, t, v) \in \text{tr}$, then there exists an abstract closure $\hat{c} \in \hat{\rho}(\delta, \phi(\text{calls}(\pi)))$ such that $v \in \gamma_{\text{cl}}(\{\hat{c}\})$.
- If $\text{Ret}(\pi, p, v) \in \text{tr}$, then there exists an abstract closure $\hat{c} \in \hat{C}(p, \phi(\text{calls}(\pi)))$ such that $v \in \gamma_{\text{cl}}(\{\hat{c}\})$.

The theorem highlights the meaning of $\hat{\rho}$ and $\hat{C}$ as solutions of the $\phi$-CFA analysis of the closed program $t_0$ considered in the empty context. First, the theorem tells us that for every $\beta$-reduction event in the trace of the analysed program, there is a corresponding entry in the global environment $\hat{\rho}$ that contains an abstract value $\hat{c}$ that contains the value used as argument during that $\beta$-reduction. Second, for every return event in the trace of the program, there is in the cache $\hat{C}$ a corresponding entry that contains an abstract value $\hat{c}$ that contains the returned value as reported by the event.

The proof of Theorem 4.6 proceeds by unfolding Def. 4.4 and exploiting the order relations and the concretization functions of the Galois connections.

## 5 Beyond the Finite State Abstraction

In this section, we deviate from the finite state approximation methodology usually applied in CFAs, and introduce an abstract domain for closures, that is recursively defined, and whose values can have unbounded depths. To ensure the convergence of the analysis, we use a widening operator, as prescribed by the abstract interpretation theory, that makes ascending chains stationary. We obtain the $\text{V}\text{CFA}$ analysis.

### 5.1 Abstract Closures with Widening

The abstract domain is derived from the domain of Def. 3.13. The environments in that previous domain could contain infinite sets of closures. In this new domain, we only consider finite sets of closures, and moreover, we enforce that there is at most one abstract environment per function. The abstract closures $c^\sharp \in \text{Clos}^\sharp$ are thus either a finite map from functions to their closing abstract environment, or the element $\top$, that represents the set of all closures from §3.5.

**Definition 5.1** (Abstract Closures).

\[ \text{Clos}^\sharp \triangleq (\forall \text{fin} \triangleright \text{fin}) + \{\top\} \quad \text{fin} \ni x \rightarrow \text{Clos}^\sharp \]

We define the union of abstract closures as follows:

**Definition 5.2** (Union of closures).

\[ \mathcal{T} \cup_{\text{clos}} m \triangleq m \quad \mathcal{U} \cup_{\text{clos}} \mathcal{T} \triangleq \mathcal{T} \cup \mathcal{U} \cup_{\text{clos}} m \triangleq \mathcal{T} \]

\[ m_1 \cup_{\text{clos}} m_2 \triangleq \lambda v. \begin{cases} m_1(v) & \text{if } v \in \text{dom } m_1 \cap \text{dom } m_2 \\ m_2(v) & \text{if } v \in \text{dom } m_1 \setminus \text{dom } m_2 \\ m_2(v) & \text{if } v \in \text{dom } m_2 \setminus \text{dom } m_1 \end{cases} \]

\[ \Gamma_1 \cup_{\text{clos}} \Gamma_2 \triangleq \lambda x. (\Gamma_1(x) \cup_{\text{clos}} \Gamma_2(x)) \]

The interesting part of the definition is for the finite maps, that represent the set of closures. The union is defined as the pointwise union of these maps.

Using solely this abstract union operator in an abstract interpreter could make the analysis diverge, because unions can build infinite ascending chains of values. Therefore, we introduce a widening operator $\text{W} \cup_{\text{clos}}$, that is more approximate than $\cup_{\text{clos}}$, and ensures that sequences of abstract values built from widenings are eventually stationary. The widening operator is defined as follows:
The different abstraction steps that lead to $\nabla$VCFAs are summarised in Fig. 3. The starting point is the abstract semantics we obtained after closure abstraction (§3.5). From there, we apply our new abstraction, that builds the new abstract values of §5.1. Then, we notice in the inclusions of Lemma 3.14 that the global environment $\rho$ is not necessary to compute the cache. So, we remove the global environment $\rho$, using a standard abstraction. Finally, we choose to only keep the value of the cache that corresponds to the whole program that is analysed, i.e. for the program $[1]p$, we only keep the entry $C(p)$. In §5.3 we present a solver that computes such a cache as an intermediate result.

We define $G(p) \doteq \gamma_{\text{clo}} \circ \gamma_{\text{env}} \circ \gamma_{\text{cache}}(p)$ and $G_{\text{clo}} \doteq \gamma_{\text{clo}} \circ \gamma_{\text{clo}} \circ \gamma_{\text{env}} \circ \gamma_{\text{cache}}(p)$ and $G_{\text{clo}} \doteq \gamma_{\text{clo}} \circ \gamma_{\text{env}} \circ \gamma_{\text{cache}}(p)$ and At the top of the abstraction stack, the following semantic inclusions hold:

\[
\begin{align*}
\mathcal{T} \to (X \xrightarrow{\text{fin}} \varphi(\text{Clos}^d)) \to \text{Clos} \\
\mathcal{T} \to (X \xrightarrow{\text{fin}} \varphi(\text{Clos}^d)) \to \text{Clos} \\
\mathcal{T} \to (X \xrightarrow{\text{fin}} \varphi(\text{Clos}^d)) \to \text{Clos} \\
\mathcal{T} \to (X \xrightarrow{\text{fin}} \varphi(\text{Clos}^d)) \to \text{Clos} \\
\end{align*}
\]

Figure 3. Abstraction steps to obtain $\nabla$VCFAs.

The inclusions resemble a big-step evaluator that computes sets of values. For variables, a lookup is performed in the environment. For functions, a singleton containing an abstract closure is returned. When functions are found at an application point, each of them is analysed, and the union of their analysis results is returned.

5.3 A Widening-Based Control Flow Analysis

In this section, we give some elements about the implementation of VCFAs, that is publicly available as a companion artefact. The core of the analyser is concentrated in the following function, named analyze:

Definition 5.5 (V-analysis).

\[
\begin{align*}
\text{analyze}(\text{analyze}_{\text{rec}})(\text{iw}, \delta, \Gamma^d, [x]p) & \doteq \Gamma^d(x) \\
\text{analyze}(\text{analyze}_{\text{rec}})(\text{iw}, \delta, \Gamma^d, [x \cdot t]p) & \doteq \langle[x \cdot t], \Gamma^d_{[\text{live}(x, t)]} \rangle \\
\text{analyze}(\text{analyze}_{\text{rec}})(\text{iw}, \delta, \Gamma^d, [[t_1]p_1, [t_2]p_2]p) & \doteq \\
\text{let } V_1 = \text{analyze}_{\text{rec}}(\text{false}, \delta, \Gamma^d, [t_1]p_1) \text{ in } \\
\text{let } V_2 = \text{analyze}_{\text{rec}}(\text{false}, \delta, \Gamma^d, [t_2]p_2) \text{ in } \\
\text{let } iw' = \text{maximal}(\delta(\phi)) \text{ in } \\
\text{analyze}(\text{analyze}_{\text{rec}}(iow', \phi(\delta(\phi)), (t_1^d, x: V_2), [t_2]p_2)) \\
\text{let } V_3 = \text{analyze}_{\text{rec}}(\text{true}, \delta, \Gamma^d, [t_1]p_1) \text{ in } \\
\text{let } V_4 = \text{analyze}_{\text{rec}}(\text{true}, \delta, \Gamma^d, [t_2]p_2) \text{ in } \\
\text{let } iw' = \text{maximal}(\phi(\delta(\phi))) \text{ in } \\
\text{analyze}(\text{analyze}_{\text{rec}}(iow', \phi(\delta(\phi)), (t_1^d, x: V_2), [t_2]p_2)) \\
\text{analyze} : (\text{bool} \times D \times D \times T) \to \text{Clos}^d \doteq \mu(\text{analyze})
\end{align*}
\]

The program analyze is executed using a top-down solver, i.e. a higher-order function $\mu$ of the form $(\alpha \to \beta) \to (\alpha \to \beta) \to (\alpha \to \beta)$, that computes a function $\mu(f)$ such that $f(\mu(f)) = f(\mu(f))$. The functional $f$ is written using the open recursion style, that was also highlighted in [4]. The actual computation $\mu(f)(x)$ on some argument $x$ is performed on demand. A simple top-down solver memoizes the calls to $f$ together with the so-far computed outputs, and iterates until it finds a post-fixpoint: it computes a cache of the calls, that is similar to the cache structure used in CFAs.

For this paper, we implemented a simple, non-optimised top-down solver, that we extended so that input widening can be demanded by the client function $f$, using the boolean argument $iw$, as we explain later in the section. More efficient top-down solvers, where computation is incremental, have already been described in the literature [1, 5, 38].

Our analyser is parameterised by a projection function $\phi$, that is required to have a finite orbit:
Definition 5.6 (Finite orbit function). We say that $\phi$ has a finite orbit, if there is a set $S$, called the set of maximal elements, such that:

- $S$ is finite, and
- for any sequence $(\rho_n)_n$ of annotations from the program, the sequence $(\delta_n)_n$ defined by $\delta_0 = \varepsilon$ and $\delta_{n+1} = \phi(\delta_n, \rho_n)$ eventually enters $S$ and then remains in $S$, i.e. there exists $n_0$ such that for every $n \geq n_0$, $\delta_n \in S$.

The finite orbit property is, for instance, satisfied by $\phi = \lfloor \cdot \rfloor_k$, where the maximal elements are the paths of length $k$.

Other choices for $\phi$ are possible, such as the function that keeps the first elements of a path $\delta$ until an element with $k$ occurrences is found, and removes the subsequent elements. We name this strategy $k^*$ in the remainder of the document.

As a counter-example, the identity function does not satisfy the finite orbit property.

The function named maximal in our code tests whether an element belongs to the set of maximal elements of $\phi$.

The argument $iw$ of the analyser controls whether input widening must be performed by the solver. When confronted with a recursive call $\text{analyze}_{rec}(\text{true}, \delta, t, \varepsilon)$—i.e. when input widening is demanded by the client—the top-down solver searches for previous calls with the arguments $\delta$ and $t$ and $\Gamma^\delta$, and computes the widening of those $\Gamma^\delta$, together with $\Gamma^\delta$. This new, widened environment, is then used as argument to actually perform the recursive call.

The termination of the algorithm is ensured by the combination of two facts. First, the top-down solver performs widening for the outputs of the function. To keep the results accurate enough, widening on outputs is performed only when the solver detects a cycle; the domain’s union is used otherwise. Second, the inputs are widened when $iw = \text{true}$. Thus, it is the responsibility of the client function—here, the function $\text{analyze}$—to ensure that enough widenings on inputs are demanded to ensure convergence. Therefore, the termination of the analysis is obtained thanks to the cooperation between the top-down solver and its client function.

The first two recursive calls on the sub-terms $\{t_1\}^{p_1}$ and $\{t_2\}^{p_2}$ make the term argument decrease, and are thus not a source of divergence. The only source of non-termination are the recursive calls on the body of the computed closures. There are two cases for such calls: if $\phi(\delta p)$ is not maximal, then the number of annotations $p'$ that can be added before the sequence of call sites reaches the maximal set decreases. This ensures convergence in this case. Otherwise, $\phi(\delta \rho)$ is maximal, and remains in the set of maximal elements, that is finite. Widening on $\Gamma^\delta$ is performed, and the stationarity of widening sequences implies the termination of the analyser.

The call site paths that we use in the analyser are only used as elements of a heuristic to guide the widening strategy. They are not part of the abstract values, as it is the case in $k$-CFA. Thus, these paths need no specific semantic justification for the soundness of the analysis to be proved.

6 Experimental Results

We implemented $k$-CFA and $\nabla$CFA in OCaml [23], so as to compare their precision and cost. For the comparison between the different analyses to be fair, we removed the computation of the cache from $k$-CFA (so that only the global environment and the abstract value for the whole program are computed), following what we did in §5. We extended the two analyses to support booleans and integers, so that more examples can be analysed. The prototype analysers and the suite of program tests are publicly available in the artefact that accompanies the article.

With these experiments, we want to show that the area of the CFA design space we have uncovered is worth exploring more thoroughly: the experimental results that we obtain on standard examples extracted from the literature [8, 14, 18, 22, 27, 42] are encouraging us in pursuing this research direction. Our goal is not to show that $\nabla$CFA is better than existing CFAs, and more realistic benchmarks, e.g. measures on the impact of optimisations for compilers for functional languages, would be required to do so.

We provide in Table 1 an experimental comparison of the standard 0-CFA, the $\phi$-CFA with the two strategies of limiting paths to the last call site (1-CFA) and the one limiting to at most one occurrence of call sites (1*-CFA). We also compare with our widening-based analysis $\nabla$CFA, using the same two strategies (1-\nabla CFA and 1*-\nabla CFA). We are thus able to observe both the impact of the choice of $\phi$, and of the choice of standard CFA versus $\nabla$CFA.

We perform the following measurements: we count how many states are needed for the top-down solver to explore the abstract call graph (column “S”), and how many edges this call graph contains (column “E”). These two measures are independent of the quality of our implementation: this graph remains the same, however incremental or efficient the solver is. The third measure is the number of iterations that are needed to find a post-fixpoint (column “Iter”). Because our solver does not try to avoid unnecessary recomputations, this measure can be seen as an upper bound of the iterations that an optimised solver would perform. Lastly, the fourth measure (column “Result”) is the obtained abstract value, that we compare for precision, taking 1-CFA as a baseline.

The main takeaways from the experiments are twofold:

1. 1*-CFA generally yields better results than 1-CFA, because information loss on context sensitivity only happens when recursion is involved. For all but one program (church), 1*-CFA improves over 1-CFA in terms of precision. Moreover, the sizes of the call graphs for 1*-CFA are generally on par with those of 1-CFA, and so are the number of necessary iterations.
2. 1*-\nabla CFA generally yields better results than 1*-CFA and 1-CFA, in particular on programs that involve arithmetic computations, because classic CFAs cannot exploit expressive numeric domains such as intervals.
The use of widening generally makes the analysis converge faster but returns a less precise result. The fact that we lose precision with
\[ \text{CFA} \] only in a few cases is indication that widening can be used with benefit here.

The \text{hmca\star} examples from [14]—\text{hmca} stands for Heintze McAllester—show the expected blow-up of 0-\text{CFA}. As expected, 1-\text{CFA} performs better than 0-\text{CFA} on these examples, and gives the most accurate result. Remarkably, the other analyses explore the exact same graphs and therefore give the same results. In particular, the 1\textsuperscript{st} strategy incurs no performance penalty and \text{VCF}A does not degrade precision.

One advantage of \text{VCF}A is that it removes the finiteness constraint on the height of the abstract domain, and thus allows the use of more expressive domains, such as intervals. This benefit is visible in several examples: with \text{VCF}A, the factorial \text{fact} is shown to return a result that is greater than 1, and the 91 function of McCarthy \text{mc91} is shown to produce a result that is above 91. This is the best precision that can be achieved using intervals. This level of precision is not reachable by finite-height domains.

The examples \text{sat}, \text{sat3} and \text{sat4} are boolean satisfiability tests, that are applied to a boolean formula encoded as a function. Both 1-\text{CFA} and 1-\text{VCF}A fail to achieve the best result because the depth of the call stack is statically bounded. In contrast, 1\textsuperscript{st}-\text{CFA} and 1\textsuperscript{st}-\text{VCF}A compute the best result—i.e. the formula is satisfiable—because the call stack is only bounded for \textit{recursively} called program points.

The programs \text{ack\_cps}, \text{mc91\_cps}, \text{tak\_cps} recursively produce a continuation—a higher-order value. Classic \text{CFA} is able to show that the three examples produce integers. \text{VCF}A analyses, however, fail to keep information on the results of the continuations, and are not able to prove that the outputs must be integers. This is due to the fact that our abstract domain for closures cannot represent recursively defined sets of closures, whereas the directions used in \textit{k-}\text{CFA} can express such solutions. Exploring ways to recover more precision is left for future work. We could for instance perform a narrowing pass, or design a more expressive domain for closures, that keeps information about the results of functions—a sort of function summary—or use a relational domain such as the one of [30], that keeps relations between inputs and outputs of functions.

7 Related Work

Control flow analysis for the lambda calculus was developed by Jones [19]. Shivers [41, 42] proposed a control flow analysis for Scheme programs in continuation-passing style and introduced the notion of \textit{k-}\text{CFA} in which flow information is given relative to a context which represents an abstraction of the state. Sestoft [39] developed an analysis for computing the flow of closures in higher-order functional programs. The constraint-based formulation of \text{CFA} was introduced by Falsberg [34] and developed further by Nielsen and Nielson [31–33]. In their \textit{infinitary control flow analysis}, they propose a constraint-based framework from which they show how to obtain different kinds of \textit{k-}\text{CFA} by varying the notion of context. In that article, they leave it as an open
problem to relate the infinitary CFA to a collecting semantics of an operational semantics using abstract interpretation.

Shivers [42] outlines the proof of correctness of a control flow analysis for a CPS-based intermediate representation of Scheme. The proof is based on a non-standard denotational semantics which, in addition to the program’s result, computes a cache for each call site. This cache contains the identifiers of the lambda expressions called at that call site. From this semantics, it is possible to obtain 0-CFA and 1-CFA as abstract interpretations.

Jones and Rosendahl [21] give a denotational semantics for a higher-order functional language based on minimal function graphs [20]. This semantics computes a subset of the graph of a function (i.e., a set of (argument, result) pairs) that are necessary and sufficient to evaluate a given function call. This semantics is then abstracted in order to obtain a closure analysis that approximates the control flow of the program. The minimal function graphs could be obtained in our approach, by exploiting the return events that are labelled with call annotations—these events were removed by the first abstraction steps of §3.

Midtgaard and Jensen show how to use the principles of abstract interpretation to systematically derive control flow analyses from collecting semantics induced by abstract machines. They obtained context-insensitive analyses—akin to 0-CFA—for continuation-passing style [26] and for direct-style programs in ANF [27] based on the CESK machine.

Van Horn and Might [15] apply abstract interpretation to the internal state representation of a series of abstract state machines. This results in “abstract machines” that compute an over-approximation of control flow and other intensional information about an execution. In machines with store-allocated continuations, control flow analysis becomes the problem of abstracting the store.

Darais et al. [4] demonstrate that the “abstracting abstract machines” approach carry over to more high-level definitional interpreters that are not expressed as state machines. In particular, they show that this approach can reconstruct the CFA2 control flow analyses [44, 45] based on push-down structures that also computes precise return information.

Trace partitioning [12, 24, 36] is a technique that can increase the precision of analyses, by exploiting the execution traces of a program to create a partition of its abstract states. We can view the call site paths used as keys in the environment and in the cache of k-CFA as a mean to partition the abstract states: k-CFA computes an environment and a cache for every call site path. We obtained these paths as abstractions of the traces, which is consistent with the trace partitioning approach. Our functions \( \phi \) identify several contexts, and we use them to define context sensitivity policies. A similar approach is followed in [37, Chap. 8.2], where instances—timestamps that are used to differentiate instances of formal parameters as in the AAM approach—are abstracted using Galois connections.

8 Conclusions and Future Work

We have proposed a substitution-based small-step operational semantics for the \( \lambda \)-calculus, that produces a trace of the control flow events that take place during reduction. We have devised a series of abstractions which, when applied to the trace-based semantics, derive \( k \)-CFA by abstract interpretation. Based on the obtained abstract interpretation, we have produced a semantic justification for the constraint-based presentation of \( k \)-CFA.

We have also employed abstract interpretation to define the \( \nabla \)CFA analysis, a novel control-flow analysis that utilises non-finite domains, and takes advantage of widening to ensure termination of the analyser. We have shown that \( \nabla \)CFA can compute more precise results than those provided by \( k \)-CFA analyses, especially when numeric domains are involved. Our experiments show that using widening in CFAs is not only possible but also brings benefits.

Using the same approach, we think \( m \)-CFA [10, 29] could be obtained using a different abstraction on traces, that would keep frames instead of call sites. The question remains open whether we could also derive the more recent pushdown CFAs [6, 7, 11, 44, 45]. This could be achieved possibly by employing more precise abstractions. For example, we have not exploited so far the order in which events occur, nor have we used the contents of call annotations, that record in the calling contexts which functions were called and on which arguments. This extra information is likely to help us justify the well-bracketed aspect of pushdown analyses.

While the experimental results for \( \nabla \)CFA are encouraging concerning precision, further study is necessary to measure how the analysis performs on larger, real-world programs, and how it compares to pushdown-based analyses. To answer these questions, we need to improve the performance of our analyser. A natural target for improvement is to make our top-down solver incremental, so that unnecessary re-computations are avoided. Another improvement would be to use a more expressive abstract domain for closures, that keeps information on function results and would help the widening operator lose less information.

We have based our semantic development on a semantics of traces. This idea could be pushed further, to analyse other intentional properties of programs, such as effect analysis, or complexity analysis. Moreover, we could also enrich the traces with the inputs of the program—an approach similar to the analysis of input-output relations [30]. This would result in a relational control-flow analysis that detects which functions are called at a given program point, depending on the inputs of the program.

References


